

Amendments to the Drawings:

The attached replacement drawing sheets include new FIGS. 1, 2 and 3. FIG. 2 and 3 depict the steps of the claimed method.

REMARKS

Claim Status

Claims 1-9 are currently pending, with claims 1, 8 and 9 being in independent form. The specification has been amended. New, replacement drawings are submitted. Claims 1-9 have been amended. Support for the amendments to the claims may be found, for example, at pg. 1, lines 9-12, pg. 2, lines 33-34 and pg. 8, line 12 to pg. 9, line 25 of the specification as originally filed. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Information Disclosure Statement

The Examiner has indicated on the Form 1449A ("Information Disclosure Statement by Applicant") attached to the Office Action that the reference identified as A. J. Menezes "Handbook of Applied Cryptography, Block Ciphers", Handbook of Cryptography, CRC Press Series on Discrete Mathematics and its Applications, pgs. 559-560, Boca Raton, FL, CRC Press, 1997 US listed on the Information Disclosure Statement (IDS) filed on August 8, 2006 has not been considered. (A line is drawn through this reference.) A new IDS is submitted concurrently herewith to resubmit this reference for the Examiner's consideration. Entry and acknowledgment that the new IDS and the reference cited therein have been entered and considered is requested.

Overview of the Office Action

The drawings have been objected to for failure to show every feature of the invention specified in the claims. Withdrawal of this objection is in order, as explained below.

Claims 1-9 have been objected to based on a minor informality. Withdrawal of this objection is also in order, as explained below.

Claim 8 and 9 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Withdrawal of this rejection is also in order, as explained below.

Claim 9 stands rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. Withdrawal of this rejection is also in order, as explained below.

Claims 8 and 9 stand rejected under 35 U.S.C. §112, second paragraph, as indefinite for failure to particularly point out and claim the subject matter which applicants regard as the invention. Withdrawal of this rejection is also in order, as explained below.

Claims 9 stands rejected under 35 U.S.C. §102(b) as anticipated by U.S. Patent No. 6,772,331 (“*Hind*”). Claims 1-8 stand rejected under 35 U.S.C. §103(a) as unpatentable over *Hind* in view of U.S. Pub. No. 2003/0210789 (“*Farnham*”).

Applicants have carefully considered the Examiner’s rejections, and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now pending in the present application are patentable over the cited art.

Descriptive Summary of the Prior Art

Hind discloses “[a] method and system for enabling wireless devices to be paired or permanently associated by a user or a network administrator” (see Abstract).

Farnham discloses “a method of establishing a secure communications link between a mobile terminal of a mobile communications system and a server” (see paragraph [0012]).

Summary of the Subject Matter Disclosed in the Specification

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

The specification discloses a certification method that uses a public key certification authority and involves a mobile terminal identified on a mobile telecommunications network in which the mobile terminal is configured to receive messages encrypted by a public certification key. The claimed method comprises generating, at the mobile terminal, the public certification key. The public certification key is acquired at a telecommunications network entity (which is a part of the mobile telecommunications network) from the mobile terminal via a network call on the mobile telecommunications network. The mobile terminal is authenticated at the telecommunications network entity by a party authentication process which is implemented in a standard telephone call on the mobile telecommunications network. The public certification key and an associated authentication result are then supplied to the public key certification authority.

The claimed method provides an advantageous way to certify a public key that is used in a mobile terminal via a simpler and more robust registration process. The claimed invention advantageously relies on the existing architecture of a mobile telecommunications network on which a mobile terminal is identified, and benefits from the security procedures traditionally implemented in the architecture to identify and authenticate mobile terminals identified on the telecommunications network (see pg. 8, lines 12-18 of the specification as originally filed).

The claimed invention thus permits a reduction of the traditional complexity of the certification process and, more particularly, facilitates the registration of the mobile terminal which is required to authenticate the terminal to deliver a public key certificate.

Amendments Addressing Informalities

The Examiner has stated that “[the] drawings must show every feature of the invention specified in the claims. Therefore, the method of claims 1-7, specifically, the manipulation of the data and keys must be shown or the feature(s) canceled from the claim(s). Furthermore, nothing of the authentication of claim 2 is disclosed in the drawings as well”.

In response to this objection to the drawings, applicants submit herewith new FIGS. 2 and 3 that respectively show the steps associated with the manipulation of data and keys, and the authentication process of claim 2. FIG. 1 has been revised solely to add a figure number. In addition, applicants have amended the specification to incorporate a description of new FIGS. 2 and 3. Support for new FIGS. 2 and 3 may be found, for example, in independent claim 1 and dependent claim 2 of the application. No new matter has been added. Entry of new FIGS. 2 and 3 and revised FIG. 1 is respectfully requested.

The Examiner has also stated that claim 1 lacks antecedent basis for “that public key”, the public key”, “the terminal” and “the network entity”, and that the phrase “with a view” in claim 3 is an awkward phrase. In response to these objections, applicants have amended claims 1 and 3 in a self-explanatory manner. Withdrawal of the objections to the claims is deemed to be in order.

Patentability of the Independent Claims under 35 U.S.C. §112

The Examiner has stated that claims 8 and 9 are unclear because the “written description merely discloses that the mobile generates a key pair (private/public)... Even though the specification discloses the known method of authentication in a GSM network it is unclear whether the applicant is [using] this method to obtain the key pair... The claim language for

obtaining the key pair is generating. Generating implies some type of calculation or computation to derive a key from some other data”.

The Examiner has additionally stated that claims 8 and 9 do not provide written support for generating a key, and that claim 9 lacks enablement because the “claim matter does not enable proper encryption for which the invention is described in the specification.

In response to these rejections, applicants have amended claim 8 to recite means in the telecommunications network entity for acquiring a public certification key generated by the mobile terminal via a network call on the mobile telecommunications network”. Claim 9 has been amended to clarify that the key that is used is that produced by the mobile terminal itself. Specifically, claim 9 has been amended to recite that the key is used for encrypting messages to be received by the mobile terminal, rather than decrypting messages to be received by the mobile terminal as formerly recited in claim 9.

The claims thus define that the public key (and more generally the key pair) is generated by the mobile terminal itself. However, the claimed invention is not directed to and does not require any specific or predetermined method or algorithm for generating the public key; rather, what is important in the claimed invention is that the public key (and more generally the key pair) is generated by the mobile terminal itself. Moreover, the public key generated by the mobile terminal is unrelated to the conventional key that, as known, is dedicated for use in telephone calls and generated during a normal or standard GSM authentication procedure.

Withdrawal of the Section 112, first and second paragraph rejections is deemed appropriate.

Patentability of Independent Claim 9 under 35 U.S.C. §102

Independent claim 9 has been amended to recite, *inter alia*, means for sending a key produced by the mobile terminal to a certification authority by a network call via a telecommunications network entity of the mobile telecommunications network such that said key produced by the mobile terminal becomes a public certification key which is used for encrypting messages to be received by the mobile terminal”. Thus, independent claim 9 has been amended to clarify that the key produced by the terminal is used to encrypt messages to be received by the terminal. No new matter has been added.

The Examiner (at pg. 8 of the Office Action) asserts that:

Hind teaches a mobile communications terminal for producing at least one key for decrypting messages received by the terminal (col. 9, lines 65-67); and

means for sending said key to a certification authority by means of a network entity so that said key becomes a public key (col. 10, lines 5-10).

Applicants disagree that *Hind* teaches the expressly recited limitations of now amended independent claim 9.

Hind (col. 9, line 66 to col. 10, line 2) explains that “the device 1003 generates the public/private key pair itself 1110 and immediately stores its private key in protected storage 1115. In this case 1003's private key is never transmitted to anyone”. *Hind* (col. 10, lines 3-14) additionally explains that the “[d]evice 1003 establishes a secure or non-secure connection 1120 with the administration server and transmits 1125 only its public key to the administration server 1001. The administration server 1001 still performs the same steps of putting the public key and device identifier into a certificate request, securely transmitting the data to the Certificate Authority (CA) 1005 so that the CA can generate a digitally signed certificate 1050' using its private key and transmit the signed certificate back to the administration server 1001, and

transmitting the signed certificate to the device 1003 over a secure or insecure connection for storage there in any suitable memory location as described in FIGS. 1A and 1B”. *Hind* thus teaches that the encryption is performed by the Certificate Authority using its private key.

Hind fails to expressly teach or suggest how the Certification Authority securely authenticates the device prior to delivering a certificate for a public key associated with this device. *Hind* explains that the CA generates a digitally signed certificate using its private key and transmits the signed certificate back to the administration server. Independent claim 1, on the other hand, recites *at least* “a public certification key which is used for encrypting messages to be received by the mobile terminal”. *Hind* fails to teach or suggest this limitation. Independent claim 9 is therefore patentable over *Hind* for at least this reason.

In view of the foregoing, amended independent claim 9 is not anticipated by *Hind*. Reconsideration and withdrawal of the rejection of claim 9 under 35 U.S.C. §102 are thus deemed to be in order, and early notice to that effect is solicited.

Moreover, by virtue of the above-discussed differences between the recitations of claim 9 and the teachings of *Hind*, and the lack of any clear motivation for modifying *Hind* to achieve applicants’ claimed invention, independent claim 9 is likewise deemed to be patentable over *Hind* under 35 U.S.C. §103.

Patentability of Independent Claims 1 and 8 under 35 U.S.C. §103

Independent claim 1 has been amended to recite the steps of “acquiring, at a telecommunications network entity of the mobile telecommunications network, said public certification key from the mobile terminal via a network call on the mobile telecommunications network; authenticating, at the telecommunications network entity, the mobile terminal by a

party authentication process which is implemented in a standard telephone call on the mobile telecommunications network; and supplying the public certification key and an associated authentication result to the public key certification authority. Independent claim 8 has been correspondingly amended. Support for the amendments may be found, for example, at pg. 1, lines 9-12 and pg. 8, line 12 to pg. 9, line 25 of the specification as originally filed. No new matter has been added.

The Examiner (at pg. 4 of the Office Action) has acknowledged that *Hind* fails to teach or suggest that “the mobile terminal authenticates itself to the network prior to the certification,” as recited in independent claim 1, and cites *Farnham* for this feature.

Applicants, however, contend that no combination of *Hind* and *Farnham* achieves the subject matter of independent claims 1 and 8. There is simply nothing in *Hind* and/or *Farnham* with respect to the certification method of now amended independent claim 1 and the mobile telecommunications system of claim 8 that implements the claimed certification method. Indeed, there is nothing whatsoever in *Hind* or *Farnham* about simplifying and/or reducing the complexity of the conventional public key certification process for a mobile terminal in the manner achieved by applicants’ claimed invention.

Hind (Abstract, lines 1-3) describes a method for enabling wireless devices to be paired or permanently associated by a user or a network administrator. *Hind* (Abstract, lines 3-6) additionally describes the use of public key cryptography, machine unique identifiers and device certificates to establish a secure channel and associate the devices with each other.

Hind (col. 7, lines 59-65) explains that “[t]he preferred embodiment of the present invention assigns a certificate to each device containing the proposed radio module. The exemplary certificate described contains the device’s unique 48-bit IEEE (MAC) address

(although any unique identifier could be used equally effectively), the device's public key, a validity period, and a signature from a Certificate Authority". *Hind* thus teaches that a certificate is assigned to each device, where the certificate is signed by a Certification Authority. *Hind* fails to expressly teach or suggest how the Certification Authority securely authenticates the device before delivering a certificate for a public key associated with the device. More particularly, *Hind* fails to teach or suggest the step of "acquiring, at a telecommunications network entity of the mobile telecommunications network, said public certification key from the mobile terminal via a network call on the mobile telecommunications network," as recited in now amended independent claim 1 and correspondingly recited in now amended independent claim 8.

The Examiner's proffered analysis posits that the administration server described at columns 9 and 10 of *Hind* corresponds to applicants' claimed network entity. However, within the meaning and scope of the claimed invention, applicants' disclosed network entity is not only a device that is connected to a mobile telecommunications network and that communicates over this network, but is an element of the mobile telecommunications network architecture which is involved in the authentication of mobile terminals connected to the mobile telecommunications network. Consequently, *Hind* fails to teach or suggest the step of "authenticating, at the telecommunications network entity, the mobile terminal by a party authentication process which is implemented in a standard telephone call on the mobile telecommunications network," as recited in now amended independent claim 1 and correspondingly recited in now amended independent claim 8.

Hind also fails to teach or suggest that the Certification Authority is provided with the public key and the associated result of an authentication process. Rather, *Hind* (col. 9, lines 37-43) explains that "[a]t 1055 the administration server 1001 establishes a secure connection to a

Certificate Authority 1005 and sends 1060 the certificate request 1050 that was prepared for mobile device 1003 to the Certificate authority whereupon the Certificate Authority 1005 signs 1065 and returns 1070 the certificate signed with the Certificate Authority's private key". *Hind* thus teaches that only the public key and a device identifier are transmitted by the administration server to the Certification Authority. The device identifier of *Hind* is a parameter that was previously transmitted by the device to the administration server (see, e.g., col. 9, line 22). The device identifier of *Hind* is not obtained by an authentication process as recited in now amended independent claims 1 and 8. *Hinds* thus fails to teach or suggest the step of "supplying the public certification key and an associated authentication result to the public key certification authority," as recited in now amended independent claim 1 and correspondingly recited in now amended independent claim 8.

Farnham, on the other hand, discloses a method for generating via the Diffie-Hellman protocol a session key that is used to establish secure communications between a mobile terminal and a server. *Farnham* teaches the use of a PKI session key transport mechanism to transport a session key between the mobile terminal and the server, where the PKI transport mechanism uses asymmetric cryptographic techniques (see paragraphs [0031] to [0033]). *Farnham* fails to teach or suggest anything whatsoever with respect to the generating step of now amended independent claim 1, as well as the corresponding limitation of now amended independent claim 8. Moreover, there is no teaching or suggestion in *Farnham* of the acquiring, authenticating and supplying steps recited in now amended independent claim 1 and correspondingly recited in now amended independent claim 8.

Farnham is directed to generating a session key for establishing secure communications between a terminal and a server. However, *Farnham* fails to disclose anything whatsoever for

simplifying the public key certification process for a mobile terminal. Applicants' claimed invention, on the other hand, advantageously provides such a simplified solution for the public key certification process for a mobile terminal. *Hind* and *Farnham*, individually or in combination, thus fail to teach or suggest the express recitations of now amended independent claims 1 and 8.

By virtue of the above-discussed differences between the recitations of independent claims 1 and 8 and the teachings of *Hind* in combination with the teachings of *Farnham*, and the lack of any clear motivation for modifying the reference teachings to achieve applicants' claimed invention, independent claims 1 and 8 are deemed to be patentable over *Hind* and *Farnham* under 35 U.S.C. §103(a).

Dependent Claims

In view of the patentability of independent claims 1, 8 and 9 for at least the reasons presented above, each of dependent claims 2-7 is believed to be patentable therewith over the cited art. Moreover, each of dependent claims 2-7 additionally includes features that serve to still further distinguish the claimed invention over the applied art.

Conclusion

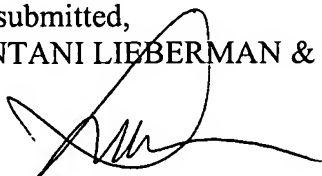
Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By



Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: December 19, 2008